



June 11, 2021

*Via Electronic Mail*

Chief Counsel's Office  
Attn: Comment Processing  
Office of the Comptroller of the Currency  
400 7th Street SW, Suite 3E-218  
Washington, DC 20219

Ms. Ann Misback  
Secretary  
Board of Governors of the Federal Reserve System  
20th Street & Constitution Avenue NW  
Washington, DC 20551

Mr. James P. Sheesley  
Assistant Executive Secretary  
Attention: Comments—RIN 3064—ZA23  
Federal Deposit Insurance Corporation  
550 17th Street NW  
Washington, DC 20429

Ms. Melane Conyers-Ausbrooks  
Secretary of the Board  
National Credit Union Administration  
1775 Duke Street  
Alexandria, VA 22314

Policy Division  
Financial Crimes Enforcement Network  
P.O. Box 39  
Vienna, VA 22183

Re: Request for Information and Comment: Extent to Which Model Risk Management Principles Support Compliance with Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Assets Control Requirements (Docket No. OCC—2020—0047; OP—1744; RIN 3064—ZA23; NCUA—2021—0007; FINCEN—2021—0004)

To Whom It May Concern:

The Bank Policy Institute<sup>1</sup> appreciates the opportunity to respond to the request for information and comment regarding the extent to which model risk management principles support compliance by

---

<sup>1</sup> The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million

banks with Bank Secrecy Act requirements and economic sanctions administered by the U.S. Department of the Treasury's Office of Foreign Assets Control.<sup>2</sup>

## I. Introduction

We note at the outset considerable work that has been done by your agencies in order to make the AML/CFT and sanctions regimes more efficient and effective—that is, to ensure that banks and other institutions responsible for detecting suspicious activity are doing so in the most effective way. This has included Treasury Department support for the recently enacted Anti-Money Laundering Act of 2020 (“AMLA”), which includes not only beneficial ownership disclosure requirements that will deter the use of anonymously owned shell companies to hide illicit behavior, but also a general mandate to the Treasury and FinCEN to foster innovation in transaction monitoring. Even aside from the legislation, however, the banking agencies and FinCEN over the past few years have taken numerous steps to rationalize the AML process, which have included, among other things, the issuance of a joint statement in August 2020 clarifying the due diligence requirements applicable to customers that may be politically exposed persons,<sup>3</sup> statements issued by FinCEN and the federal banking agencies in August 2020 setting forth BSA enforcement approaches,<sup>4</sup> a joint statement in December 2018 encouraging institutions to responsibly implement innovative AML compliance approaches,<sup>5</sup> and various revisions to the FFIEC BSA/AML Examination Manual.

---

Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

<sup>2</sup> Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, Request for Information and Comment: Extent to Which Model Risk Management Principles Support Compliance With Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Assets Control Requirements, 86 Fed. Reg. 18,978 (Apr. 12, 2021).

<sup>3</sup> Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May be Considered Politically Exposed Persons (Aug. 21, 2020), *available at* [https://www.fincen.gov/sites/default/files/shared/PEP%20Interagency%20Statement\\_FINAL%20508.pdf](https://www.fincen.gov/sites/default/files/shared/PEP%20Interagency%20Statement_FINAL%20508.pdf).

<sup>4</sup> Financial Crimes Enforcement Network, Financial Crimes Enforcement Network (FinCEN) Statement on Enforcement of the Bank Secrecy Act (Aug. 18, 2020), *available at* [https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement\\_FINAL%20508.pdf](https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf). Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Joint Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements (Aug. 13, 2020), *available at* <https://www.occ.treas.gov/news-issuances/news-releases/2020/nr-ia-2020-105a.pdf>.

<sup>5</sup> Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (Dec. 3, 2018), *available at* [https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29\\_508.pdf](https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf).

Of course, those efforts also include the recent interagency statement from the federal banking agencies, issued in consultation with FinCEN and the NCUA,<sup>6</sup> emphasizing that the Supervisory Guidance on Model Risk Management (“MRMG”)<sup>7</sup> does not have the force of law and may be interpreted flexibly as applied to AML/CFT systems. That statement, standing alone, should do much to rationalize relevant processes. That said, we welcome the current RFI as a way to amplify the Interagency Statement and ensure that it is effectively communicated both to examiners in the field and to compliance officers at institutions. We recognize that facilitating a change in direction by a broad set of examiners and institutions is always difficult, and particularly in an area that historically has been treated as one with zero tolerance for error such as this one. We also recognize that there will be challenges in ensuring that the MRMG is no longer necessarily considered binding, at least at the most risk-averse firms or by the most aggressive examiners.

For these reasons, in this letter, we emphasize why the Interagency Statement was appropriate and how we believe it will promote a banking system more difficult for bad actors to exploit, and then suggest ways that it can be implemented most effectively.

## II. Background

Tools that institutions employ to facilitate compliance with BSA/AML and sanctions requirements and expectations, including tools that are determined to be “models” for the purpose of the MRMG, frequently differ from models used by institutions for other purposes. BSA/AML and sanctions tools, for example, often rely on subjective human review of outputs, such as alerts of potential suspicious activity or sanctions hits, and information on the usefulness or practical application of the ultimate product of these tools, especially suspicious activity reports (“SARs”), is generally unavailable. These and other differences can affect, even for those BSA/AML and sanctions tools determined to be models, how institutions undertake validation, and frequently render aspects of the MRMG inapplicable in whole or in part to validation of these tools.

The Interagency Statement confirms that the objectives and structure of BSA/AML tools may differ from those of other models used by financial institutions, while also recognizing that the MRMG does not have the force and effect of law. The Interagency Statement helpfully explains that institutions have flexibility in determining how to apply the MRMG to BSA/AML tools, including those considered models. The conclusions of the Interagency Statement that institutions have discretion in applying the MRMG should apply with equal force to sanctions tools.

---

<sup>6</sup> Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance (Apr. 9, 2021) (the “Interagency Statement”), *available at* <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210409a2.pdf>.

<sup>7</sup> Board of Governors of the Federal Reserve System, Officer of the Comptroller of the Currency, Supervisory Guidance on Model Risk Management (Apr. 4, 2011), *available at* <https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf>; *see also* Federal Deposit Insurance Corporation, Adoption of Supervisory Guidance on Model Risk Management, FIL-22-2017 (June 7, 2017), *available at* <https://www.fdic.gov/news/financial-institution-letters/2017/fil17022.pdf>.

Some BPI member institutions report that they have been directed by bank examiners to apply, to the letter, the MRMG to BSA/AML and sanctions tools. Applying the MRMG to these tools without taking into account the tools' differences from models used by institutions for other purposes has often required institutions to implement processes that impose substantial costs and do not facilitate the implementation of innovative, effective, reasonably designed, and risk-based BSA/AML and sanctions compliance programs.<sup>8</sup> Accordingly, we believe that, in order to achieve the intended purposes of the Interagency Statement, it is critical that the federal banking agencies, in consultation with FinCEN and OFAC: (i) amend the FFIEC Examination Manual to include the Interagency Statement and make clear that, while the MRMG may provide helpful guidance in assessing BSA/AML and sanctions tools that are models, banks have flexibility and discretion to develop their own BSA/AML and sanctions programs, even if those programs deviate substantially from the MRMG in some program elements; and (ii) provide robust training to bank examiners on the Interagency Statement. Absent such clear guidance and examiner training, there is the real risk that examiners will continue to examine BSA/AML and sanctions tools to the letter of the MRMG, without appropriately accounting for the flexibility and discretion afforded financial institutions under the Interagency Statement in determining whether and to what extent the MRMG apply to particular BSA/AML and sanctions tools.

Properly accounting for that flexibility and discretion in exams will encourage the design and implementation of BSA/AML and sanctions programs, including underlying systems and tools, that are effective and adaptable to changes to illicit finance risks. Further, in order to ensure the intended purposes of the Interagency Statement are achieved in the longer-term, we believe that FinCEN should also reflect this flexibility and discretion in the testing methods rulemaking that the Treasury Department, in consultation with the federal banking agencies and other agencies, is required to undertake pursuant to Section 6209 of the Anti-Money Laundering Act of 2020 (the "AMLA").<sup>9</sup>

In this letter, we first describe key differences between BSA/AML and sanctions compliance tools, including those that financial institutions determine to be models, and other models used by institutions; second, comment on the particularly helpful guidance provided in the Interagency Statement; and third, explain why it is important that this guidance is reflected in examiner training and the future testing methods rulemaking.

The discussion in this letter is informed by the BSA/AML and sanctions tools currently deployed by a majority of the banking industry. We recognize that continued innovation could cause the principles in the MRMG to have greater, or lesser, applicability to certain tools used in BSA/AML and sanctions programs. We note in this regard the joint statement in 2018 that encouraged institutions to responsibly implement innovative AML compliance approaches, which has led to certain institutions beginning to explore the use of supervised machine learning in AML. The use of innovative technology in BSA/AML and sanctions tools may affect the validation processes that are appropriate for those tools. However, it will remain critical for financial institutions to retain the flexibility and discretion to determine how to best apply the MRMG. Of course, in all instances, institutions will continue to need to implement effective, reasonably designed, risk-based BSA/AML and sanctions programs. Flexibility and discretion merely empowers financial institutions to do so in a manner that accounts for an institution's

---

<sup>8</sup> BPI member institutions report a widely divergent set of approaches that they currently take in applying the MRMG to BSA/AML and sanctions tools. The descriptions in this letter represent a compilation of these various approaches, which have in many cases been implemented as a result of examiner feedback.

<sup>9</sup> 31 U.S.C. § 5318(o).

particular circumstances, including its specific systems and tools, instead of adhering to rigid validation elements that may actually impede effectiveness.

**III. BSA/AML and sanctions tools often differ substantially from the models used by financial institutions for other purposes and, as a consequence, how institutions apply the MRMG to those tools frequently differs from how they apply the MRMG to other models.**

There are often substantial differences between effective BSA/AML and sanctions tools and the types of models envisioned by the MRMG—underwriting credits; valuing exposures, instruments, and positions; measuring risk; management and safeguarding client assets; and determining capital and reserve adequacy.

Important differences include those listed below. Although one or more of these differences may apply to models used for other purposes, for example, fraud detection, it is rare that all, or even most, of these differences simultaneously apply to a non-BSA/AML or sanctions tool.

- Human intervention: BSA/AML and sanctions tools frequently rely on human review of tool-generated alerts. These alerts, whether related to potential suspicious transactions or potential sanctions concerns, are frequently neither determinative nor predictive of whether a SAR must be filed or a customer or transaction may not be accepted.<sup>10</sup> To determine whether a SAR must be filed or a transaction not accepted, investigators must manually review the alert and exercise their judgment, which often leads to the conclusion that there is no basis to file a SAR or block a transaction (i.e., that the alert is a “false positive”). Further, in some cases, an institution may decide to file a SAR regarding a transaction that was the subject of an alert for reasons unrelated to the tool scenario or rule that generated the alert (e.g., because an investigator determined information was missing or a relationship between parties could not be identified). This labor-intensive process is a poor fit for the MRMG, which requires analysis of the results generated by a model. For these BSA/AML and sanctions tools, such an analysis would include not only the alerts generated by the tools, but also the transactions and customers that did *not* generate an alert to assess whether there are “false negatives” (e.g., transactions that did not alert but on which a SAR should have been filed). Conducting such further analysis would necessarily add yet another layer of human review that would be extraordinarily inefficient. Thus, as a practical matter, it is not possible to identify all instances in which a SAR should have been filed or a transaction blocked, but was not.
- Decision accuracy information lacking: Information concerning the accuracy of decisions to, for example, file a SAR—that is, whether a “positive” result ended up being true or false—is frequently unavailable. In the case of SARs, institutions (and examiners) are generally not told whether a SAR in fact provided useful information to law enforcement or national security agencies, the ultimate users of SAR information. Although additional feedback from these agencies could be helpful for calibrating relevant bank

<sup>10</sup> Certain BSA/AML and sanctions tools may, however, provide predictive outcomes. If so, and provided the other characteristics of a model under the MRMG are present, the MRMG may have greater applicability to such tools than they do to other BSA/AML and sanctions tools.

systems, it is inconceivable that sufficient feedback would be provided on all SAR filings. Further, due to the general obligation to maintain the confidentiality of SARs, institutions may be unable to benchmark their filing decisions against external data.

- Absence of quantitative estimates or less complexity: Some BSA/AML and sanctions tools do not make quantitative estimates or predictions or are far less complex quantitatively than the types of models used in other contexts. For example, tools used for the purpose of currency transaction reporting or sanctions screening may rely on relatively simple logic to determine if a particular transaction or customer should be subject to further manual review. Such tools bear little resemblance to the complex, data-driven, quantitative decision-making models envisioned by the MRMG.<sup>11</sup>
- Thresholds set based on subjective judgments: The thresholds used for BSA/AML tools frequently must rely on the subject-matter expertise of BSA/AML personnel, including based on past investigative outcomes and views of appropriate customer segmentation. Quantitative testing methods under the MRMG frequently have little relevance to thresholds necessarily determined based on these subjective judgments.
- Need for agility: Because criminals adapt their behavior to avoid AML or sanctions screening, financial institutions must be nimble in responding to new techniques for hiding illicit cash. Such agility often is not required with respect to models used for other purposes. For example, capital regulations do not change on a daily or weekly basis, and therefore banks do not need to quickly amend the models that produce their capital levels. Moreover, because of amendments made to the BSA by the AMLA, institutions in the future may need to make changes even *more* frequently to their BSA/AML tools to meet emerging threats and typologies.<sup>12</sup>
- Lower material impact: BSA/AML and sanctions tools typically have a lower potential to materially impact an institution's financial condition or business decisions than other models within scope of the MRMG. For example, the consequences of a good faith error in calculating capital requirements are far more likely to have a material impact on an institution's financial condition or the business decisions it makes than a good faith error in calibrating a suspicious transaction monitoring tool.

Due to these and other potential differences between BSA/AML and sanctions tools and other models within the scope of the MRMG, the elements that the MRMG describes for “verify[ing] that models are performing as expected, in line with their design objectives and business uses,”<sup>13</sup> often do

---

<sup>11</sup> Accordingly, consistent with the MRMG, some institutions treat these more qualitative or less complex tools as outside the scope of the MRMG but nonetheless subject them to rigorous control processes. See MRMG, at 3 (“While outside the scope of this guidance, more qualitative approaches used by banking organizations—i.e., those not defined as models according to this guidance—should also be subject to a rigorous control process.”).

<sup>12</sup> For example, under the BSA, as amended, the Secretary of the Treasury, in consultation with the Attorney General, federal functional regulators, relevant state financial regulators, and relevant national security agencies, are required to begin publishing on a periodic basis AML/CFT priorities. 31 U.S.C. § 5318(h)(4).

<sup>13</sup> MRMG, at 9.

not apply to validation of BSA/AML and sanctions tools. The MRMG's three core elements are: (i) an evaluation of conceptual soundness, which "involves assessing the quality of the model design and construction"; (ii) ongoing monitoring, which "confirms that the model is appropriately implemented and is being used and is performing as intended"; and (iii) outcomes analysis, which involves "a comparison of model outputs to corresponding actual outcomes."<sup>14</sup> We describe below how some institutions have sought to address each of these elements in validating BSA/AML and sanctions tools, and the extent to which certain elements may be inapplicable or require tailoring.

*Conceptual soundness.* Consistent with the MRMG, institutions generally evaluate the conceptual soundness of their BSA/AML and sanctions tools. These evaluations may involve the following activities, depending on the type of tool being evaluated or tested:

- Documentation review: Determining whether a tool's rule and alert definitions and configurations are identified and sufficiently explained and justified, which frequently requires the review of detailed documentation not only from an application vendor but also from the financial institution's BSA/AML or sanctions personnel.
- Transaction verification: Verifying that the tool covers and evaluates all appropriate transactions and customers.
- Risk assessment review: Evaluating whether the tool's configurations are consistent with the institution's risk assessment methodology.
- Data review: Reviewing all data inputs for the tool, including their quality, and confirming that the institution has mapped, extracted, transformed, and correctly loaded the data inputs from their respective source systems.
- Watchlist filtering: Validating that the institution has properly configured watchlist criteria and that the tool receives all relevant information needed to generate alerts.

*Ongoing monitoring.* In contrast to conceptual soundness, ongoing monitoring of BSA/AML and sanctions tools frequently differs significantly from other models within the scope of the MRMG. Under the MRMG, ongoing monitoring includes process verification and benchmarking, which entails comparing the results produced by a model against targets and tolerances established during model development.

BSA/AML and sanctions tools are ill-suited to the sort of benchmarking comparison contemplated by the MRMG. As noted above, there is generally no external data against which to compare alerts or other results produced by BSA/AML and sanctions tools, especially those tools designed to assist in the determination of whether to file a SAR. Further, although "challenger models" may be used to test other types of models, it is unlikely that an institution could effectively implement such a tool to test a BSA/AML or sanctions tool. Integrating such an additional BSA/AML or sanctions tool into an institution's systems, and confirming it is operating as intended, would require a substantial amount of time and resources that could be more effectively deployed to other areas of a BSA/AML or sanctions program. Further, because BSA/AML and sanctions monitoring tools generally review every

---

<sup>14</sup>

MRMG, at 11-13.

customer or every transaction to generate alerts for ultimate disposition, it would be impractical to review the alerts produced by two separate tools. In addition, because tool thresholds frequently rely on subjective inputs, once the “challenger” tool is configured to align with the tool being tested, the objective of benchmarking will be largely defeated. Finally, to the extent tools differed in the alerts they generated, institutions would be put in the difficult position of trying to decide which tool is “more right.”

Accordingly, institutions frequently rely more on process verification for ongoing monitoring of BSA/AML and sanctions tools. Such process verification may include monitoring of alerts and other model outputs and sampling of customer and transaction information that did not generate an alert to assess potential “false negatives.” However, for the reasons described above, even a review for false negatives generally requires human review, and, as a result, institutions cannot be certain they have identified all potential false negatives. That notwithstanding, institutions may face significant adverse legal consequences for failing to detect and report on particular customers or transactions, potentially including those not identified by a BSA/AML or sanctions tool.

*Outcomes analysis.* The third MRMG core element, outcomes analysis, is also a poor fit for BSA/AML and sanctions tools. As mentioned above, it may be impossible to compare the outputs generated by BSA/AML and sanctions tools, which are not generally designed to predict the future, to actual outcomes (*e.g.*, whether a SAR in fact provided useful information to law enforcement). As a result, instead of outcomes analysis, institutions generally perform a broader analysis of how tools are functioning. This analysis may include—depending on the design of an institution’s BSA/AML or sanctions program and the characteristics of a particular tool—to varying degrees the following activities, among others:

- Rule relevance: Assessing potentially unproductive tool rules, for example, based on how many rules are never triggered or, when triggered, are always overridden in the course of human review of the relevant alert.
- Distribution analysis: Determining whether the distribution of alerts is logical in light of typical customer transaction activity and the institution’s view of its overall risk profile.
- Monitoring output: For suspicious transaction monitoring tools, for example, monitoring information about the number of SARs that are filed based on alerts generated.
- Management reporting: Analyzing how alerts and other outputs, including for example SARs, are incorporated into management reports, and how such reports are reviewed for accuracy, communicated to management, and subsequently archived.<sup>15</sup>
- Output maintenance: Reviewing how reports are created and maintained, and how tool output is archived for reporting and ongoing monitoring purposes.

---

<sup>15</sup> Review of management reporting is especially important with respect to filed SARs in light of the requirement that a bank notify the board or a designed committee of each filed SAR. 12 C.F.R. §§ 21.11(h), 208.62(h), 353.3(f), 748.1(c)(4).

- Internal Controls: Evaluating tool configurations and whether applicable tool strengths, weaknesses, and limitations are understood by users, including what the tool is, and is not, designed to detect.
- Screening configuration: For sanctions tools, assessing the lists incorporated in the tool, the data points used in screening, the ability of the tool to detect variations (e.g., in birthdates or names or through “fuzzy” matching), and the use and maintenance of any “whitelisting.”

Because any given BSA/AML or sanctions tool is only one piece of an institution’s overall BSA/AML or sanctions program, these or other analyses of outcomes form part of a broader assessment of how an institution’s tools, both individually and collectively, contribute to the overall effectiveness of the program.

\* \* \* \* \*

Because there may be significant challenges in applying the MRMG to BSA/AML and sanctions tools, BPI members report widely divergent approaches in how they apply the MRMG in this context. Several institutions report that they consider all or almost all BSA/AML and many sanctions tools to be models under the MRMG. Others consider far fewer BSA/AML tools and no or almost no sanctions tools to be models. Member institutions also report differences in how they apply the MRMG to BSA/AML and sanctions tools that are determined to be models. Some institutions permit substantial tailoring of the MRMG elements for validation of BSA/AML and sanctions tools; some institutions have a process to grant waivers for certain MRMG-related procedures; and some institutions do not meaningfully differentiate how they apply the MRMG elements to models, whether they are BSA/AML or sanctions tools or other models. Member institutions also differ in the extent to which they permit BSA/AML and sanctions tools to be expedited into production.

We believe that the differences in application of the MRMG to BSA/AML and sanctions tools arise because, as described above, BSA/AML and sanctions tools used today are frequently substantially different from other models to which the MRMG apply.

#### **IV. BPI appreciates the Interagency Statement addressing how the MRMG relates to systems used by institutions to assist in complying with BSA/AML requirements.**

As noted above, the Interagency Statement helpfully recognizes that institutions have discretion and flexibility to determine how to apply the MRMG to BSA/AML tools. The following aspects of the statement are especially important in this context:

- Emphasizing that the MRMG does not have the force and effect of law;
- Recognizing that there may be important differences between BSA/AML tools and models used by institutions for other purposes, including due to a potential emphasis on coverage over efficiency and a lack of information about realized accounts that can be used for testing and performance monitoring;
- Acknowledging that validation of BSA/AML tools may take these differences into account;

- Describing that institutions may determine whether a particular BSA/AML tool is a model for the purpose of the MRMG and, for those tools that are models, how to best apply model validation processes;
- Clarifying that the MRMG does not provide “‘templates’ or requirements,” but instead provide useful information for an institution’s consideration;
- Stating that the MRMG “provide[s] flexibility,” including to permit institutions to “update BSA/AML models quickly in response to the evolving threat environment and to implement innovative approaches”; and
- Providing that there is no requirement that institutions “have duplicative processes for complying with BSA/AML regulatory requirements” or “perform duplicative independent testing activities, including model validation, to ensure compliance with BSA/AML program requirements.”

Given the similarities between BSA/AML and sanctions tools, the conclusions of the Interagency Statement, including the discretion and flexibility that institutions are recognized to have, should apply with equal force to sanctions tools.

To achieve the intended purposes of the Interagency Statement, we believe it to be critical that the federal banking agencies, in consultation with FinCEN and OFAC, update the FFIEC Manual to include the Interagency Statement and then train examiners on how to apply it.

**V. The federal banking agencies, working with FinCEN, should ensure that the FFIEC Manual and examiner training reflect the flexibility and discretion afforded in the Interagency Statement, and FinCEN should do the same in the testing methods rulemaking required under the AMLA.**

**A. The FFIEC Manual and examiner training should include the Interagency Statement.**

BPI member institutions report that in many cases they have rigidly applied the MRMG elements to BSA/AML and sanctions tools as a result of examiner feedback. In the institutions’ experience, examiners have frequently treated the MRMG as binding and applicable to a wide range of processes, including BSA/AML and sanctions tools for which the MRMG is a poor fit. Applying the MRMG in this way has imposed significant costs on institutions, which deploy resources to implement associated governance structures and demonstrate MRMG compliance, neither of which is an efficient means to generate actionable recommendations or to optimize a BSA/AML program’s effectiveness.

The Interagency Statement makes clear that there is no requirement to apply the MRMG in this way, and that institutions instead have flexibility and discretion in applying the MRMG, especially in the context of BSA/AML tools. Examiner training would help facilitate alignment among the agencies and examiners and across financial institutions, including personnel in business units, BSA/AML and sanctions compliance, model risk management, and internal audit. The training should communicate the key aspects of the Interagency Statement described in Part IV above, including that the MRMG is not binding and that institutions may determine which BSA/AML tools are models and, for those tools that are models, whether and how to apply the MRMG.

With respect to BSA/AML tools, the training should also emphasize the unique function and position of the BSA Officer, who is expressly responsible for coordinating and monitoring day-to-day BSA/AML compliance, and who must regularly report to the board and senior management regarding the BSA/AML program. The BSA Officer should be recognized as empowered, subject to appropriate oversight and escalation to the board and senior management, to make decisions on how BSA/AML tools, including those determined to be models, are implemented, including how to respond to validation feedback. Further, the training should reiterate that neither a BSA/AML program overall, nor the models and other tools used in that program, is required to be “perfect,” as has been recognized in recent revisions to the FFIEC Manual.<sup>16</sup> Accordingly, there should not be a regulatory expectation that institutions will identify every false negative; rather, the goal is for a BSA/AML program, including the tools used in that program, to be reasonably designed on the basis of risk. Similarly, the training should emphasize the absence of any requirement that institutions “have duplicative processes for complying with BSA/AML regulatory requirements” or “perform duplicative independent testing activities, including model validation, to ensure compliance with BSA/AML program requirements.”<sup>17</sup> Personnel performing model validation are model experts and often not BSA/AML experts. Accordingly, model validation should focus on design and whether a model is functioning as intended and should not serve as a substitute for the BSA Officer’s judgment as to what constitutes an effective BSA/AML program or for independent review of the program.

Although the Interagency Statement does not expressly apply to sanctions tools, for the reasons described above, the statement’s conclusions should apply the same to those tools. As with BSA/AML tools, the MRMG is frequently a poor fit with sanctions tools. However, the lack of a statement from the banking agencies addressing the application of the MRMG to sanctions tools makes it particularly critical that examiners receive training specifically addressing the flexibility and discretion that institutions have in applying the MRMG to sanctions tools. Without explicit guidance, there is a greater potential that examiners and institutions will continue to view the MRMG as necessarily applicable to sanctions tools. Examiner training therefore should emphasize that the principles of the Interagency Statement apply to sanctions tools. The training should also make clear, as described above with respect to BSA/AML tools, that sanctions tools are not required to be perfect or identify every false negative and that institutions are not required to deploy duplicative processes or duplicative independent testing activities with respect to these tools.

Providing training to encourage alignment around the flexibility and discretion that institutions have in determining the extent to which the MRMG applies to BSA/AML and sanctions tools would provide at least two important benefits. *First*, institutions would be better able to appropriately allocate BSA/AML and sanctions program resources. As noted above, applying the MRMG to BSA/AML and sanctions tools for which the MRMG is a poor fit has imposed substantial costs on institutions. Flexibility to determine how the MRMG is applied, in contrast, would improve an institution’s ability to determine how it allocates program resources. Regardless of how an institution validates a particular BSA/AML or sanctions tool, including one determined to be a model, the institution remains subject to the BSA’s requirement that it maintain a reasonably designed, risk-based BSA/AML program, and OFAC’s similar expectation with respect to the institution’s sanctions program. Discretion to determine

---

<sup>16</sup> FFIEC Manual, Developing Conclusions and Finalizing the Exam, at 1 (Mar. 2020) (“Minor weaknesses, deficiencies, and technical violations alone are not indicative of an inadequate BSA/AML compliance program and should not be communicated as such.”).

<sup>17</sup> Interagency Statement, at 3-4.

whether and how the MRMG informs development of a BSA/AML or sanctions tool, including one determined to be a model, would enable institutions to allocate resources more efficiently, consistent with recent proposals, including by FinCEN, that would encourage the design and implementation of effective BSA/AML programs.<sup>18</sup>

For example, BPI member institutions report that applying MRMG validation approaches to sanctions screening tools has pushed institutions to spend significant resources on documenting detection or non-detection of typographically, linguistically, and commercially unrealistic permutations of sanctioned party names (*e.g.*, “NORth K0Re@”). As another example, BPI member institutions report that applying the MRMG, including in light of related examiner feedback, has made it difficult to turn off or discontinue tool scenarios or rules, even in circumstances in which the scenarios or rules have led to the filing of very few SARs. This difficulty arises due to a concern that a decrease in coverage will allow for false negatives, regardless of whether the institution has determined that one or more different scenarios or rules is more appropriate on the basis of risk and better at covering relevant typologies.

Both of these examples generate substantial opportunity costs in focusing on inefficient activities—the overwhelming majority of sanctions-related “hits” relate to reasonable name variations, not improbable permutations—and updates and changes to scenarios and rules may be more effective, especially as new threats and typologies emerge and are identified. In both cases, resources could be more effectively allocated to other activities, including proactive analytics and customer due diligence in the first example and more productive rules and scenarios in the second. Where applying the MRMG leads to counterproductive or unproductive results, an institution should be able to determine, by considering the nature of a tool and on the basis of risk, whether or how to apply the MRMG.

It is important to note that, for BSA/AML or sanctions tools, flexibility and discretion in determining how to apply the MRMG need not cause institutions to disregard the MRMG’s core elements in some areas. BPI member institutions report that, today, the MRMG has greater applicability to certain BSA/AML and sanctions tools, such as where a tool includes alerting criteria that are driven by complex statistical analyses.

*Second*, greater flexibility in this context will enable institutions to be more proactive in responding to changes in applicable illicit finance risks. When the MRMG applies, institutions generally include a substantial amount of rigor in their model validation processes, increasing the rigidity of these processes. BPI members appreciate that the MRMG can improve the effectiveness of models used in other contexts, such as with respect to credit, capital, or liquidity modeling. However, procedures rigidly implementing the MRMG substantially increase the time and resources required for model validation, including for model changes. For those BPI member institutions that define “model” broadly to include many BSA/AML tools and generally require *all* such models to undergo validation prior to being put into production, substantial delays arise in updating BSA/AML or sanctions tools to address new typologies. Delays can be due to testing procedures, preparation of required documentation, education of validators, or other reasons.

Institutions should have discretion to determine whether to undertake pre-implementation validation with respect to a particular tool or whether, consistent with the institution’s risk appetite, it

---

<sup>18</sup> See Financial Crimes Enforcement Network, Anti-Money Laundering Program Effectiveness, 85 Fed. Reg. 58,023 (Sept. 17, 2020).

would be more effective to implement the tool, potentially as a pilot, and perform validation only at a later time when more information is available about how the tool has performed. This discretion would enable institutions to implement BSA/AML and sanctions tools, and changes to those tools, more quickly. As a result, institutions would be better able to respond to emerging typologies and, where such typologies are identified, to provide useful information about them to law enforcement and national security authorities. Greater flexibility in determining when to undertake validation would also facilitate the introduction of more innovative BSA/AML and sanctions tools, including those that complement existing tools. Encouraging innovation in this context would also be consistent with objectives recognized in the AMLA of “effectively encourag[ing] and support[ing] technological innovation in the area of [AML] and [CFT]” and “reduc[ing], to the extent practicable, obstacles to innovation,”<sup>19</sup> as well as the 2018 joint statement discussed above, which encourages institutions to responsibly implement innovative AML compliance approaches.

**B. FinCEN should recognize the flexibility that applies to validation of BSA/AML tools in the testing methods rulemaking required under the AMLA.**

Section 6209 of the AMLA requires that the Secretary of the Treasury, in consultation with the federal banking agencies and other agencies, issue a rule specifying standards by which institutions are to test technology and related technology internal processes. These standards may include, among other things, “risk-based testing” and “an emphasis on using innovative approaches such as machine learning or other enhanced data analytics processes.”<sup>20</sup>

To ensure the intended purposes of the Interagency Statement are achieved in the longer-term, to enable institutions to better tailor their validation processes on the basis of risk, and to encourage innovation, this rulemaking should provide that institutions have the flexibility and discretion discussed above to determine whether and how to validate BSA/AML tools. This rulemaking should also take into account the unique aspects of BSA/AML tools, including those described above, should permit institutions to undertake BSA/AML tool testing in a manner that improves overall BSA/AML program effectiveness, and should consider differences that have developed among institutions based on whether and to what extent they have already implemented the MRMG with respect to BSA/AML tools.

\* \* \* \* \*

The Bank Policy Institute appreciates the agencies’ consideration of its comments. If you have any questions, please contact the undersigned by phone at 202-589-1935 or by email at [Angelena.Bradfield@bpi.com](mailto:Angelena.Bradfield@bpi.com).

Respectfully submitted,



Angelena Bradfield  
Senior Vice President, AML/BSA, Sanctions & Privacy  
Bank Policy Institute

<sup>19</sup> See AMLA, § 6207.

<sup>20</sup> 31 U.S.C. § 6318(o).